U.S. Department of Justice

National Security Division

SECRET//COMINT//ORCON,NOFORN

Washington, D.C. 20530

November 20, 2007

MEMORANDUM FOR THE ATTORNEY GENERAL

THROUGH: THE ACTING DEPUTY ATTORNEY GENERAL

FROM: Kenneth L. Wainstein
Assistant Attorney General
National Security Division

CC: Steven G. Bradbury
Principal Deputy Assistant Attorney General
Office of Legal Counsel

SUBJECT: Proposed Amendment to Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States (S//SI)

PURPOSE: To Recommend Attorney General Approval Pursuant to Executive Order 12333 of a Proposed Amendment to Procedures Governing the National Security Agency's Signals Intelligence Activities (S//SI)

SYNOPSIS: The Secretary of Defense seeks your approval of proposed Department of Defense Supplemental Procedures Governing Communications Metadata Analysis ("Supplemental Procedures"). The Supplemental Procedures, attached at Tab A, would clarify that the National Security Agency (NSA) may analyze communications metadata associated with United States persons and persons believed to be in the United States. These Supplemental Procedures would amend the existing procedures promulgated pursuant to Executive Order

Classified by: [redacted]
Reason: [redacted]
Declassify on: 20 November. 2032

12333.[1] That Order requires the NSA to conduct its signals intelligence activities involving the collection, retention, or dissemination of information concerning United States persons in accordance with procedures approved by the Attorney General. Accordingly, changes to these procedures, such as those proposed here, also require your approval. We conclude that the proposed Supplemental Procedures are consistent with applicable law and we recommend that you approve them.[2] (S//SI)

The communications metadata that the NSA wishes to analyze—which relates to both telephone calls and electronic communications—is dialing, routing, addressing, and signaling information that does not concern the substance, purport, or meaning of the communication. The procedures divide communications metadata into two categories: telephony metadata and electronic communications metadata. Telephony metadata includes such information as the telephone numbers of the calling and the called party. Electronic communications metadata includes such information as the e-mail address and the Internet protocol (IP) address of the computer of the sender and the recipient. This communications metadata has been obtained by various methods, including pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801, et seq., and resides in NSA databases.[3] NSA plans to analyze this data primarily using a technique known as "contact chaining." Contact chaining involves the identification of telephone numbers, e-mail addresses, or IP addresses that a targeted telephone number, IP address, or e-mail address has contacted or attempted to contact. Through the use of computer algorithms, NSA creates a chain of contacts linking communicants and identifying additional telephone numbers, IP addresses, and e-mail addresses of intelligence interest. On the basis of prior informal advice of the Office of Intelligence Policy and Review, NSA's present practice is to "stop" when a chain hits a telephone number or address believed to be used by a United States person. NSA believes that it is over-identifying numbers and addresses that belong to United States persons and that modifying its practice to chain through all telephone numbers and addresses, including those reasonably believed to be used by a United States person, will yield valuable foreign intelligence information primarily concerning non-United States persons outside

[1] *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons* (DOD Reg. 5240.1-R)(Dec. 1982)(approved by the Attorney General on Oct. 4, 1982)("DOD Procedures") and its Classified Annex. The proposed Supplemental Procedures would clarify Procedure 5 of the DOD Procedures and its Classified Annex. (U)

[2] This memorandum was prepared in consultation with the Office of Legal Counsel. (U)

[3] This memorandum assumes that the NSA's initial acquisition of the information it wishes to analyze was lawful. (U)

the United States. It is not clear, however, whether NSA's current procedures permit chaining through a United States telephone number, IP address or e-mail address. (S//SI)

We conclude that the proposed communications metadata analysis, including contact chaining, is consistent with (i) the Fourth Amendment; (ii) FISA; and (iii) the electronic surveillance provisions contained in Title 18 of the United States Code. The Supplemental Procedures are also consistent with the requirements of Executive Order 12333. (S//SI)

As you consider this proposed change, you should be aware of the following:

(1) *Congressional Oversight.* At the request of the Secretary of Defense, NSA briefed the Select Committee on Intelligence of the United States Senate and the Permanent Select Committee on Intelligence of the United States House of Representatives on this proposed change before the Secretary signed the Supplemental Procedures.

(2) *Oversight of NSA's Activities Under the Supplemental Procedures.* Because NSA has in its databases a large amount of communications metadata associated with persons in the United States, misuse of this information could raise serious concerns. The General Counsel of NSA has provided a letter, attached at Tab B, describing how NSA will oversee access to and use of this data and committing to report annually to you on NSA's communications metadata program. As part of this reporting, NSA undertakes to inform the Department of "the kinds of information that NSA is collecting and processing as communications metadata." Particularly as technology changes, this requirement is important because the legal standards governing metadata are quite different from those governing the contents of a communication. We believe that the oversight and reporting regime that this letter describes is a reasonable one, and it informs our recommendation that you approve the Supplemental Procedures. (S//SI)

(3) *The Central Intelligence Agency's (CIA) Interest in Conducting Similar Communications Metadata Analysis.* On July 20, 2004, the General Counsel of CIA wrote to the General Counsel of NSA and to the Counsel for Intelligence Policy asking that CIA receive from NSA United States communications metadata that NSA does not currently provide to CIA. The letter from CIA is attached at Tab C. Although the proposed Supplemental Procedures do not directly address the CIA's request, they do resolve a significant legal obstacle to the dissemination of this metadata from NSA to CIA. (S//SI//NF)

(4) *Department of Defense's (DOD) Interest in Allowing Other DOD Entities to Have Access to this Data and to Conduct Similar Analysis.* The DOD's General Counsel's Office has informed us that, in the future, other DOD entities may wish to obtain and analyze communications metadata using the same rules that NSA uses to do so. The proposed Supplemental Procedures do not apply to these other DOD entities, but you should be aware that

such a request may be forthcoming. As part of its oversight responsibilities, the National Security Division will be briefed by DOD concerning what these other DOD entities are doing, or are seeking to do, in this area before approving any such request. (S//SI)

DISCUSSION: (U)

The Fourth Amendment (U)

The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. This provision protects against the unreasonable search and seizure of the contents of a communication in which a person has a reasonable expectation of privacy. *See Katz v. U.S.*, 389 U.S. 347 (1967). We conclude that a person has no such expectation, however, in dialing, routing, addressing, or signaling information that does not concern the substance, purport, or meaning of communications.[4] We reach this conclusion with respect to "metadata"

---

[4] As an initial matter, we note that the analysis of information legally within the possession of the Government is likely neither a "search" nor a "seizure" within the meaning of the Fourth Amendment. *See, e.g., Jabara v. Webster*, 691 F.2d 272, 277-79 (6th Cir 1982) (holding that the disclosure of information by an agency that lawfully possessed it to another agency does not implicate the Fourth Amendment); Memorandum for the Attorney General from Theodore B. Olson, Assistant Attorney General, Office of Legal Counsel, *Re: Constitutionality of Certain National Security Agency Electronic Surveillance Activities Not Covered Under the Foreign Intelligence Surveillance Act of 1978*, at 59 (May 24 1984) ("Olson Memorandum") ("Traditional Fourth Amendment analysis holds that once evidence is constitutionally seized, its dissemination or subsequent use raises no additional Fourth Amendment question."). As noted, we assume for the purpose of this memorandum that the NSA has lawfully acquired the information it wishes to analyze. Nevertheless, the Olson Memorandum went on to consider the limits on the subsequent use of information when assessing the constitutionality of NSA's surveillance activities under the Fourth Amendment. *See id.* In an abundance of caution, then, we analyze the constitutional issue on the assumption that the Fourth Amendment may apply even though the Government has already obtained the information lawfully. (S//SI)

associated with both telephone calls and electronic communications.[5] (S//SI)

The Supreme Court has held that there is no reasonable expectation of privacy in telephone numbers dialed because a caller must convey the numbers to the telephone company to complete the call. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). In *Smith*, the Court concluded that the installation of a pen register was not a "search" within the meaning of the Fourth Amendment, and thus that no warrant was required to collect such information. *Id.* at 745-46. This conclusion followed from the Court's previous holding in *U.S. v. Miller*, 425 U.S. 435 (1976), that an individual has no Fourth Amendment privacy interest in information released to a third party and later conveyed by that third party to a governmental entity. *Id.* at 440. Accordingly, it is well settled that there is no reasonable expectation of privacy in the telephony metadata the NSA proposes to analyze.[6] (S//SI)

Likewise, there is no reasonable expectation of privacy in electronic communications metadata. For Fourth Amendment purposes, courts have considered e-mails to be analogous to telephone calls and to letters sent through the postal system. *See U.S. v. Charbonneau*, 979 F. Supp 1177, 1184 (S.D. Ohio 1997); *U.S. v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996). Following the same approach as *Smith*, courts have consistently held that the Fourth Amendment is not implicated when the Government gathers information that appears on mail covers, including the name and address of the addressee and of the sender, the postmark, and the class of mail. *See U.S. v. Choate*, 576 F.2d 165, 174 (9th Cir. 1978); *U.S. v. DePoli*, 628 F.2d 779 (2nd Cir. 1980); *U.S. v. Huie*, 593 F.2d 14 (5th Cir. 1979)(per curiam). *See also Vreeken v. Davis*, 718 F.2d 343, 347-48 (10th Cir. 1983) (concluding that a mail cover, which records information about the sender and recipient of a letter, is "indistinguishable in any important respect from the pen register at issue in *Smith*"). And courts have consistently found that individuals do not have a reasonable expectation of privacy in information pertaining to the use of electronic media that

---

[5] It is important to note that this memorandum addresses only those types of metadata specifically identified in the Supplemental Procedures. As described above, NSA is required to report regularly to the Department on new types of information that it is treating as "metadata." If NSA does so, we will evaluate whether such new information also falls outside the Fourth Amendment. (S//SI)

[6] *Smith* continues to be cited by the Supreme Court and lower courts for the proposition that acquisition of telephone numbers does not implicate the Fourth Amendment. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 33 (2001); *U.S. Telecom Commission v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000). (U)

does not reveal the substantive content of a communication.[7] The electronic communications metadata the NSA proposes to analyze—dialing, routing, addressing or signaling information—is identical in all material respects to the information deemed not to implicate the Fourth Amendment in these lines of cases. (S//SI)

Thus, when interpreting the Fourth Amendment, the courts have drawn a consistent distinction between the substantive content of the communications (found to be protected in *Katz*) and the non-content information (found to be unprotected in *Smith*, *Miller* and a number of lower court cases). The communications metadata implicated by the proposed Supplemental Procedures is limited to dialing, routing, addressing, or signaling information and is defined specifically to exclude any information that concerns the substance, purport or meaning of the communication. Thus it falls clearly within the second, unprotected category of information. We conclude, therefore, that there is no reasonable expectation of privacy in this metadata and that the communications metadata analysis proposed by NSA does not implicate the Fourth Amendment. (S//SI)

FISA's Electronic Surveillance Provisions (U)

To fall within FISA's coverage of "electronic surveillance," an action must satisfy one of the four definitions of that term. None of these definitions cover the communications metadata analysis at issue here.[8] (S)

---

[7] *See Thygeson v. U.S. Bancorp*, WL 2066746 (D. Or. 2004) (noting the distinction between the website addresses at issue there, in which an employee had no reasonable expectation of privacy, and the contents of websites visited or e-mails sent). *See also U.S. v. Hambrick*, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion) (holding that, although in certain circumstances a person may have a privacy interest in "content information" such as the substance of an e-mail, there is no privacy interest in information provided to the ISP for purposes of establishing the account, which, according to the court, is non-content information); *U.S. v. Ohnesorge*, 60 M.J. 946 (N.M. Ct. Crim. App. 2005) (holding that there is no reasonable expectation of privacy regarding information provided to an ISP). (S//SI)

[8] As noted above, some of the metadata the NSA would analyze has been acquired pursuant to FISA and thus is subject to the minimization procedures applicable to that collection. The standard NSA FISA minimization procedures contain no restrictions that would prohibit the metadata analysis described herein. The NSA will continue to comply with these procedures, including with any restrictions on the dissemination of information. In addition, to the extent that any orders authorizing, under FISA, the collection of metadata impose minimization procedures that would restrict the metadata analysis in the manner proposed here by NSA, the NSA must continue to abide by the conditions in those orders. (S//SI)

Three of the four definitions of electronic surveillance are satisfied only when the communication is acquired "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(1), (3), (4). This statutory expectation-of-privacy requirement adopts a term of art from Fourth Amendment case law. *See, e.g., Katz*, 389 U.S. at 361 (Harlan, J., concurring). "[W]here Congress borrows terms of art . . . it presumably knows and adopts . . . the meaning [their] use will convey to the judicial mind unless otherwise instructed." *Morissette v. United States*, 342 U.S. 246, 263 (1952). The legislative history confirms the applicability of this presumption in this instance. It repeatedly adverts to constitutional standards when discussing this provision. *See, e.g.*, S. Rep. 95-701, at 37, 1978 U.S.C.C.A.N. at 4006 (noting that the provision "require[s] that the acquisition of information be under circumstances in which a person has a constitutionally protected right of privacy"); H.R. Rep. No. 95-1283, at 53 (same); S. Rep. No. 95-604, at 35, 1978 U.S.C.C.A.N. at 3937 (same). For the reasons stated above, there is no reasonable expectation of privacy in the communications metadata at issue here; therefore, NSA's proposed activity would not come within the definitions of electronic surveillance contained in subsections 1801(f)(1), (3) or (4). (S)

The fourth definition of electronic surveillance involves "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication . . . ." 50 U.S.C. § 1802(f)(2). "Wire communication" is, in turn, defined as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier . . . ." *Id.* § 1801(l). The data that the NSA wishes to analyze already resides in its databases. The proposed analysis thus does not involve the acquisition of a communication "while it is being carried" by a connection furnished or operated by a common carrier. (S//SI)

Pen Register and Trap and Trace Provisions (U)

The pen register and trap and trace surveillance provisions of FISA, 50 U.S.C. §§ 1841-1846, and of the criminal law, 18 U.S.C. §§ 3121-27, do not apply to the communications metadata analysis that NSA wishes to conduct. (S//SI)

First, for the purpose of these provisions, "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing or signaling information." 18 U.S.C. § 3127(3); 50 U.S.C. § 1841(2). When NSA will conduct the analysis it proposes, however, the dialing and other information will have been already recorded and decoded. Second, a "trap and trace device" is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information." 18 U.S.C. § 3127(4); 50 U.S.C. § 1841(2). Again, those impulses will already have been captured at the point that NSA conducts chaining. Thus, NSA's communications metadata analysis falls outside the coverage of these provisions. (S//SI)

Title III (U)

The federal criminal wiretap statute, Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510, et seq., prohibits the unauthorized "intercept[ion]" of any wire, oral or electronic communication, *id.* at § 2511(1), which is defined as the acquisition of the "contents" of the communication, *id.* at § 2510(4). It also prohibits the use and disclosure of the "contents" of such a communication if it was unlawfully intercepted. *See id.* at § 2511(1). For the purpose of these prohibitions, "contents" is defined as "information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8); *see United States* v. *New York Telephone Co.*, 434 U.S. 159 (1977) (holding that Title III does not cover the acquisition of metadata with pen registers). By its terms, the Supplemental Procedures' definition of the communications metadata to be analyzed excludes information about the substance, purport, or meaning of the communication. For this reason at least, the prohibitions of section 2511(1) do not apply to the proposed communications metadata analysis. (S//SI)

Executive Order 12333 and Related Procedures (U)

Executive Order 12333 requires the NSA to conduct its signals intelligence activities involving the collection, retention, or dissemination of information concerning United States persons in accordance with procedures approved by the Attorney General. *See id.* § 2.3; § 2.4.[9] These procedures must permit the collection, retention, and dissemination of certain types of information including foreign intelligence information in a manner that protects constitutional and other legal rights and limits the use of the information to lawful government purposes. *See id.* § 2.4. The Attorney General approved the current Department of Defense procedures and Classified Annex in October 1982. (U)

The current DOD procedures and their Classified Annex may be read to restrict NSA's ability to conduct the desired communications metadata analysis, at least with respect to metadata associated with United States persons. In particular, this analysis may fall within the procedures' definitions of, and thus restrictions on, the "interception" and "selection" of communications.

---

[9] In addition, section 2.5 of Executive Order 12333 provides that the "Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes." Because individuals have no reasonable expectation of privacy in the types of metadata at issue here, no warrant would be required to analyze this information for law enforcement purposes. In addition, the analysis of information legally within the possession of the government is likely neither a "search" nor a "seizure" within the meaning of the Fourth Amendment. *See* note 4, *supra*. Section 2.5 thus does not require the Attorney General to approve NSA's proposed analysis of communications metadata. (S)

Accordingly, the Supplemental Procedures that would govern NSA's analysis of communications metadata expressly state that the DOD Procedures and the Classified Annex do not apply to the analysis of communications metadata. Specifically, the Supplemental Procedures would clarify that "contact chaining and other metadata analysis do not qualify as the 'interception' or 'selection' of communications, nor do they qualify as 'us[ing] a selection term,' including using a selection term 'intended to intercept a communication on the basis of . . . [some] aspect of the content of the communication." Once approved, the Supplemental Procedures will clarify that the communications metadata analysis the NSA wishes to conduct is not restricted by the DOD procedures and their Classified Annex. (S//SI)

The Supplemental Procedures define the terms "communications metadata," "contact chaining," and "metadata analysis." The Supplemental Procedures also state that NSA will conduct contact chaining and other metadata analysis only for valid foreign intelligence purposes; disseminate the results of its analysis in accordance with current procedures governing dissemination of information concerning U.S. persons as set forth in Section 4.A.4 of the Classified Annex; and investigate any apparent misuse or improper dissemination of metadata and report the same to the appropriate oversight organization(s). (S//SI)

In addition, the NSA letter accompanying the Supplemental Procedures proposes a regulatory and oversight regime for the handling of communications metadata of U.S. persons. NSA states that access to communications metadata will be restricted to only those personnel with a need for this data in the performance of their official duties. Before gaining access to communications metadata, NSA or other personnel working under the authority of the Director of NSA will receive mandatory training approved by the General Counsel of NSA on the proper use of such databases and chaining tools. When logging into the electronic data system, users will view a banner that re-emphasizes key points regarding use of the data, chaining tools, and proper dissemination of results. NSA will also create an audit trail of every query made in each database containing U.S. communications metadata, and a network of auditors will spot-check activities in the database to ensure compliance with all procedures. In addition, the NSA Oversight and Compliance Office will conduct periodic super audits to verify that activities remain properly controlled. Finally, NSA will report any misuse of the information to the NSA's Inspector General and Office of General Counsel for inclusion in existing or future reporting mechanisms related to NSA's signals intelligence activities. (S//SI//OC,NF)

NSA also states it will report any changes to this oversight regime to the Assistant Attorney General for the National Security Division, and, by October 15 of each year, will submit a report to the Attorney General regarding the kinds of information the NSA is collecting and processing as communications metadata, NSA's implementation of its compliance procedures, and any significant new legal or oversight issues that have arisen in connection with NSA's activities described in this memorandum. (C)

As drafted, the Supplemental Procedures meet the requirements of Executive Order 12333. Together with the current approved procedures, they continue to permit the collection of foreign intelligence and other information and, as explained above, the metadata analysis will be for lawful government purposes and consistent with the Constitution and other applicable law. (S)

RECOMMENDATION: Based on the information provided by NSA and our analysis of applicable law, we conclude that there are no constitutional or statutory restrictions on NSA's proposed use of communications metadata. We therefore recommend that you approve the Supplemental Procedures. (S//SI)

(S//SI) Department of Defense Supplemental Procedures Governing Communications Metadata Analysis

Sec. 1: Purpose

(S//SI) These procedures supplement the Procedures found in DoD Regulation 5240.1-R and the Classified Annex thereto. These procedures govern NSA's analysis of data that it has already lawfully collected and do not authorize collection of additional data. These procedures also clarify that, except as stated in section 3 below, the Procedures in DoD Regulation 5240.1-R and the Classified Annex thereto do not apply to the analysis of communications metadata.

Sec. 2: Definitions

(S//SI) Communications metadata means the dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport or meaning of the communication. The two principal subsets of communications metadata are telephony metadata and electronic communications metadata.

(a) Telephony "metadata" includes the telephone number of the calling party, the telephone number of the called party, and the date, time, and duration of the call. It does not include the substance, purport, or meaning of the communication.

(b) For electronic communications, "metadata" includes the information appearing on the "to," "from," "cc," and "bcc" lines of a standard e-mail or other electronic communication. For e-mail communications, the "from" line contains the e-mail address of the sender, and the "to," "cc," and "bcc" lines contain the e-mail addresses of the recipients. "Metadata" also means (1) information about the Internet-protocol (IP) address of the computer from which an e-mail or other electronic communication was sent and, depending on the circumstances, the IP address of routers and servers on the Internet that have handled the communication during transmission; (2) the exchange of an IP address and e-mail address that occurs when a user logs into a web-based e-mail service; and (3) for certain logins to web-based e-mail accounts, inbox metadata that is transmitted to the user upon accessing the account. "Metadata" associated with electronic communications does not include information from the "subject" or "re" line of an e-mail or information from the body of an e-mail.

(S//SI) Contact chaining. Contact chaining is a process by which communications metadata is organized. It shows, for example, the telephone numbers or e-mail addresses that a particular telephone number or e-mail address has been in contact with, or has attempted to contact. Through this process, computer algorithms automatically identify not only the first tier of contacts made by the seed telephone number or e-mail address, but also the further contacts made by the first tier of telephone numbers or e-mail addresses and so on.

Sec. 3: Procedures

(a) (S//SI) NSA will conduct contact chaining and other communications metadata analysis only for valid foreign intelligence purposes.

(b) (S//SI) NSA will disseminate the results of its contact chaining and other analysis of communications metadata in accordance with current procedures governing dissemination of information concerning US persons. *See* Section 4.A.4 of the Classified Annex to Procedure 5 of DoD Regulation 5240.1-R.

(c) (U//FOUO) Any apparent misuse or improper dissemination of metadata shall be investigated and reported to appropriate oversight organization(s). *See* Procedure 15 of DoD Regulation 5240.1-R.

Sec. 4: Clarification

(S//SI) For purposes of Procedure 5 of DoD Regulation 5240.1-R and the Classified Annex thereto, contact chaining and other metadata analysis do not qualify as the "interception" or "selection" of communications, nor do they qualify as "us[ing] a selection term," including using a selection term "intended to intercept a communication on the basis of . . . [some] aspect of the content of the communication."

Robert M. Gates (signature)
Dr. Robert Gates
Secretary of Defense

10-19-07
Date

Approved by:
(signature)
Michael B. Mukasey
Attorney General
of the United States

1/3/08
Date

B

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: GC/120/06
28 September 2006

Mr. James A. Baker
Counsel for Intelligence Policy
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Jim:

(S//SI) The National Security Agency (NSA) is requesting that the Secretary of Defense and the Attorney General approve an amendment to the Classified Annex to Department of Defense Procedures Under Executive Order 12333 (May 27, 1988). That amendment would permit NSA personnel analyzing communications metadata to analyze contacts involving U.S. telephone numbers, e-mail addresses, and other identifiers. While NSA has for several years engaged in such activities, it has heretofore applied procedures in a manner that has precluded it from chaining "from" or "through" communications connections with telephone numbers and electronic communications metadata when it has had reason to believe the communications were those of U.S. persons.

(S//SI/OC,NF) NSA is committed to vigorous and effective oversight of all of its activities that affect the privacy interests of U.S. persons. With respect to the communications metadata of U.S. persons affected by this amendment, NSA wishes to inform you of the following:

1. NSA acquires this communications metadata under its authority to collect, process, and disseminate signals intelligence information under Executive Order 12333. All of the communications metadata that NSA acquires under this authority should have at least one communicant outside the United States.

2. The Oversight and Compliance Office in NSA's Signals Intelligence Directorate conducts oversight of NSA's activities involving communications metadata.

3. NSA restricts access to communications metadata to those analytic and other personnel with a need for this data in the performance of their official duties.

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify on: 20291123

4. Before NSA or other personnel working under the authority of the Director of NSA obtain access to communications metadata, such personnel will receive mandatory training, approved by the General Counsel of NSA, on the proper use of such databases and chaining tools. That training may be provided on-line. Users will complete and acknowledge the training before access. The training will highlight the sensitivity of the data and the users' obligations when accessing the data, the restriction on use of the data to foreign intelligence purposes only, and the requirement to follow required procedures when disseminating results.

5. Before accessing the data, users will view a banner, displayed upon login and positively acknowledged by the user, that re-emphasizes the key points regarding use of the data and chaining tools, and proper dissemination of any results obtained.

6. NSA creates audit trails of every query made in each database containing U.S. communications metadata, and has a network of auditors who will be responsible for spot-checking activities in the database to ensure that activities remain compliant with the procedures described for the data's use. The Oversight and Compliance Office conducts periodic super audits to verify that activities remain properly controlled.

7. NSA will report any misuse of the information to NSA's Inspector General and Office of General Counsel for inclusion in existing or future reporting mechanisms relating to NSA's signals intelligence activities.

(C) Should any of these statements change, NSA will promptly inform the Assistant Attorney General, National Security Division, U.S. Department of Justice. In this event, NSA will discuss with the Assistant Attorney General what other steps NSA should take to ensure effective oversight of communications metadata of U.S. persons.

(C) In addition, each year by October 15th, I will report to the Attorney General on (i) the kinds of information that NSA is collecting and processing as communications metadata; (ii) NSA's implementation of the steps described above; and (iii) any significant new legal or oversight issues that have arisen in connection with NSA's collection, processing, or dissemination of communications metadata of U.S. persons.

Sincerely,

Vito T. Potenza

VITO T. POTENZA
Acting General Counsel

cc: General Counsel, Department of Defense
General Counsel, Office of Director of National Intelligence
Civil Liberties Protection Officer, Office of Director of National Intelligence